

J75B-537

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-085472

(43)Date of publication of application : 30.03.1999

(51)Int.Cl. G06F 7/58
G09C 1/00
H04L 9/26

(21)Application number : 09-249109

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 12.09.1997

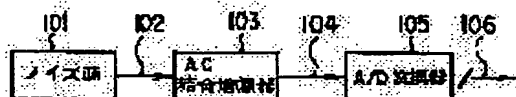
(72)Inventor : ONODERA TORU
KANEMOTO SHIGERU
SUMIYAMA SHIGEAKI

(54) PHYSICAL RANDOM NUMBER GENERATION DEVICE AND METHOD THEREFOR, AND PHYSICAL RANDOM NUMBER RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To increase the generating speed of physical random numbers and also to secure the good characteristics for the random numbers by providing the random number data based on the digital value which are converted by an A/D conversion means.

SOLUTION: Noise signals 102 which are generated from a noise source 101 due to a random event are amplified up to the conversion range of an A/D converter 105 by an AC coupling amplifier 103. Thus, the digital data are obtained and the random number data are generated from the digital data. A piece of random number data is obtained via a single conversion operation by applying the A/D conversion to the amplified signals 102 not by counting the random pulses of signals 102. Furthermore, the random number data of many bits are generated by the converter 105 and in a single A/D conversion operation. Thus, it is possible to obtain the random number data having no periodicity, to fast generate the physical random numbers and also to simplify the circuit constitution.



LEGAL STATUS

[Date of request for examination] 03.10.1997

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 2980576

[Date of registration] 17.09.1999

[Number of appeal against examiner's decision
of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2000 Japanese Patent Office

(19) 日本国特許庁 (J P)

(12) 特 許 公 報 (B 2)

(11) 特許番号

第2980576号

(45) 発行日 平成11年(1999)11月22日

(24) 登録日 平成11年(1999)9月17日

(51) Int.Cl.⁶
G 0 6 F 7/58
G 0 9 C 1/00
H 0 4 L 9/26

識別記号

6 5 0

F I

G 0 6 F 7/58
G 0 9 C 1/00
H 0 4 L 9/00

A

6 5 0 B

6 5 9

請求項の数24(全 21 頁)

(21) 出願番号 特願平9-249109
(22) 出願日 平成9年(1997)9月12日
(65) 公開番号 特開平11-85472 ✓
(43) 公開日 平成11年(1999)3月30日
審査請求日 平成9年(1997)10月3日
早期審査対象出願

(73) 特許権者 000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地
(72) 発明者 小野寺 徹
神奈川県川崎市幸区小向東芝町1番地
株式会社東芝研究開発センター内
(72) 発明者 兼本 茂
神奈川県横浜市磯子区新杉田町8番地
株式会社東芝横浜事業所内
(72) 発明者 角山 茂章
神奈川県川崎市幸区小向東芝町1番地
株式会社東芝研究開発センター内
(74) 代理人 弁理士 鈴江 武彦 (外6名)
審査官 石田 信行

最終頁に続く

(54) 【発明の名称】 物理乱数発生装置及び方法並びに物理乱数記録媒体

(57) 【特許請求の範囲】

【請求項1】 ノイズ信号を出力するノイズ源と、
前記ノイズ信号を交流結合により直流分を除去しつつ増幅するAC結合増幅手段と、
前記AC結合増幅手段により増幅された増幅ノイズ信号をA/D変換する、2ビット以上の精度を有して2ビット以上のビットデータに変換するA/D変換手段と、
前記A/D変換手段により変換された2ビット以上のビットデータを微分非直線性を改善するよう加工し、この加工データに基づいて2ビット以上の乱数データを提供
する加工手段とを備えたことを特徴とする物理乱数発生装置。

【請求項2】 前記A/D変換手段により変換されたデジタル値の平均値を、前記A/D変換前若しくは前記A/D変換後のデータに加えるオフセット調整手段を備

えたことを特徴とする請求項1記載の物理乱数発生装置。

【請求項3】 前記A/D変換手段は6ビット以上の精度を有し、変換されたデジタル値を構成する6ビット以上のビットデータのうち、上位から5ビット目以降の2つ以上のビットデータを取り出して乱数データとすることを特徴とする請求項1又は2記載の物理乱数発生装置。

【請求項4】 前記変換されたデジタル値の頻度分布が平均N、分散 σ^2 の正規分布となるとき、前記変換されたデジタル値が $N \pm \sigma$ 以上の範囲に入る場合のみを有効とすることを特徴とする請求項1乃至3記載のうち何れか1項記載の物理乱数発生装置。

【請求項5】 前記A/D変換手段が出力する2以上の前記変換されたデジタル値を加算平均する微分非直線

性改善手段を備えたことを特徴とする請求項1乃至4記載のうち何れか1項記載の物理乱数発生装置。

【請求項6】 前記A/D変換手段の入力値に微分非直線性改善用データをオフセットとして加算するとともに、前記微分非直線性改善用データに相当する改善用デジタルデータを前記A/D変換手段の出力値から減算する微分非直線性改善手段を備えたことを特徴とする請求項1乃至4記載のうち何れか1項記載の物理乱数発生装置。

【請求項7】 前記ノイズ源は、熱雑音を前記ノイズ信号として使用することを特徴とする請求項1乃至6記載のうち何れか1項記載の物理乱数発生装置。

【請求項8】 前記ノイズ源は、抵抗の熱雑音を前記ノイズ信号として使用することを特徴とする請求項1乃至6記載のうち何れか1項記載の物理乱数発生装置。

【請求項9】 前記ノイズ源は、半導体素子の熱雑音を前記ノイズ信号として使用することを特徴とする請求項1乃至6記載のうち何れか1項記載の物理乱数発生装置。

【請求項10】 前記ノイズ源は、フォトマルチプライヤの光電変換面の熱雑音を前記ノイズ信号として使用することを特徴とする請求項1乃至6記載のうち何れか1項記載の物理乱数発生装置。

【請求項11】 前記ノイズ源は、真空管の陰極より発生する熱雑音を前記ノイズ信号として使用することを特徴とする請求項1乃至6記載のうち何れか1項記載の物理乱数発生装置。

【請求項12】 前記ノイズ源は、真空マイクロ素子により発生する電子のゆらぎを前記ノイズ信号として使用することを特徴とする請求項1乃至6記載のうち何れか1項記載の物理乱数発生装置。

【請求項13】 前記ノイズ源を高温で一定に保つ恒温手段を備えたことを特徴とする請求項7乃至11記載のうち何れか1項記載の物理乱数発生装置。

【請求項14】 前記乱数データに基づくデータを表示する表示手段を備えたことを特徴とする請求項1乃至13記載のうち何れか1項記載の物理乱数発生装置。

【請求項15】 前記乱数データを用いて信号を変調する信号変調手段を備えたことを特徴とする請求項1乃至13記載のうち何れか1項記載の物理乱数発生装置。

【請求項16】 前記乱数データを用いてデータの暗号化を行う暗号化手段を備えたことを特徴とする請求項1乃至13記載のうち何れか1項記載の物理乱数発生装置。

【請求項17】 前記請求項1乃至13記載のうち何れか1項記載の物理乱数発生装置と、前記物理乱数発生装置からの乱数データをコンピュータに入力可能に構成された、前記コンピュータのデータ入出力バスとのインターフェイス手段とを備えたことを特徴とする物理乱数入力装置。

【請求項18】 前記請求項1乃至13記載のうち何れか1項記載の物理乱数発生装置と、

前記物理乱数発生装置からの乱数データをコンピュータの要求に応じてコンピュータ・ネットワークに送出可能に構成された、前記コンピュータ・ネットワークとのインターフェイス手段とを備えたことを特徴とする物理乱数入力装置。

【請求項19】 生成された乱数データを記録する記憶手段を備え、

乱数出力要求があった場合に、この要求に応じて乱数データを供給することを特徴とする請求項1乃至13記載のうち何れか1項記載の物理乱数発生装置。

【請求項20】 前記請求項1乃至13記載のうち何れか1項記載の物理乱数発生装置により生成された乱数データを記録したことを特徴とする物理乱数記録媒体。

【請求項21】 記録された乱数データについての検定方法及び又は検定結果を記録したことを特徴とする請求項20記載の物理乱数記録媒体。

【請求項22】 ノイズ源からノイズ信号を出力するステップと、

前記ノイズ信号を交流結合により直流分を除去しつつ増幅するAC結合増幅ステップと、

前記AC結合増幅ステップにおいて増幅された増幅ノイズ信号をA/D変換する、2ビット以上の精度を有して2ビット以上のビットデータに変換するA/D変換ステップと、

前記A/D変換ステップにより変換された2ビット以上のビットデータを微分非直線性を改善するよう加工し、この加工データに基づいて2ビット以上の乱数データを提供するステップとを有することを特徴とする物理乱数発生方法。

【請求項23】 前記A/D変換手段の入力信号が変換範囲を超えたときに無効とし、変換範囲を超えずに変換されたデジタル値を乱数データとすることを特徴する請求項1乃至4記載のうち何れか1項記載の物理乱数発生装置。

【請求項24】 前記加工手段は、補正信号をD/A変換して前記A/D変換手段への入力前の値に加算し、かつ、前記補正信号を前記A/D変換手段の出力から差し引くことで乱数データに加工する手段、

又は、前記A/D変換手段から別々に出力されるA/D変換値同士、若しくは前記A/D変換手段の出力と前記A/D変換の出力以外のランダムなデータを、加算(排他OR)して乱数データに加工する手段、

の何れかであることを特徴する請求項1乃至16記載のうち何れか1項、又は請求項19項、若しくは請求項23項記載の物理乱数発生装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は物理乱数発生装置及び方法並びに記録媒体、更に詳しくは汎用のコンピュータからパソコンやゲーム機のような民生レベルまで幅広い分野へ適用される物理乱数発生装置及び方法に関するものである。

【0002】

【従来の技術】物理乱数とは、自然界のランダム現象を利用して作成された乱数のことを言い、代表的なランダム現象としては、放射線の発生や熱雑音のゆらぎ等が挙げられる。

【0003】従来の物理乱数発生装置では、ノイズ源として放射線や熱雑音を用い、ノイズ源から発生するランダム・パルスの発生間隔または発生頻度を測定している。

【0004】例えば、単位時間当たりの放射線の発生個数を何度も測定し、測定値の頻度分布を作成すると平均 N 、標準偏差 $N^{1/2}$ の正規分布に近づく。すなわち、100回の測定を行った場合、そのうち99回は、 $N-3N^{1/2}$ から $N+3N^{1/2}$ のいずれかの値になる。測定値の頻度分布は正規分布なので、このまま正規分布乱数として用いることができるが、一般的には分布が一樣な方が便利なが多いため正規分布を一樣乱数に変換する必要がある。

【0005】そこで、従来装置では、正規分布から一樣乱数を得るために、計数結果の最下位桁の値だけを用いて頻度分布形状に依存しない乱数としている。さらに、得られた計数値の最下位桁として1ビットの値を用いることにより、計測結果を偶数または奇数の2通りに分類することができ、 N が十分に大きければ各々の発生頻度は50%になり、乱数としての性質が向上する。

【0006】従来装置では、このような1ビットの乱数データ発生回路を複数個用意することにより、多ビットの乱数データを発生している。このような従来技術は、例えば石田正次氏の「モンテカルロ法と乱数」(科学基礎論研究17, 2, 29(1965))等に記載されている。

【0007】

【発明が解決しようとする課題】しかし、上述したような従来の一樣な物理乱数発生方法では、計数ノイズ信号から乱数データを得るためには、 N (100~200)個のノイズ信号を計数しなければならないため、1個の乱数を発生するために多くの時間が必要となるという課題がある。

【0008】また、計数結果として1つのノイズ源から発生できる乱数データは1ビットのため、たとえば、計算機が扱う最小単位であるバイト単位の乱数データを発生するためには、8つの互いに相関のないノイズ源と8系統の乱数発生回路が必要になる。これは装置の小型化・低価格化を実現するために解決されるべき課題である。

【0009】このような課題のため、物理乱数発生装置から発生する乱数データを用いた膨大なシミュレーションを行う場合、計算機にいかにも高速なCPUを搭載しても、計算結果が得られる時間が乱数発生速度に依存するためシミュレーションの高速化を実現できないという状況となっていた。

【0010】また、1バイトの乱数を発生するために8系統のノイズ源と処理回路が必要となるため装置が大きくなり、これが低価格化を阻害し、物理乱数発生装置の普及を阻む要因となつている。

【0011】一方、高速かつ安価な従来から物理乱数発生装置が実現されれば、シミュレーション、知能関連の研究、ネットワーク上のセキュリティー研究等の科学技術計算分野や、通信機器分野(通信データのセキュリティー、変調の暗号化等の通信機器分野のみならず、パチンコ台の出玉確率、一般のゲーム機等のゲーム機分野等)にも利用されることが考えられる。

【0012】本発明は、このような実情を考慮してなされたもので、物理乱数発生速度を向上するとともに、乱数として良質な特性を有する物理乱数を提供し、さらには汎用のコンピュータからパソコンやゲーム機のような民生レベルまで幅広い分野への適用をできるようにした物理乱数発生装置及び方法、物理乱数入力装置並びに物理乱数記録媒体を提供することを目的とする。

【0013】

【課題を解決するための手段】上記課題を解決するために、請求項1に対応する発明は、ノイズ信号を出力するノイズ源と、ノイズ信号を交流結合により直流分を除去しつつ増幅するAC結合増幅手段と、AC結合増幅手段により増幅された増幅ノイズ信号をA/D変換する、2ビット以上の精度を有して2ビット以上のビットデータに変換するA/D変換手段と、前記A/D変換手段により変換された2ビット以上のビットデータを微分非直線性を改善するよう加工し、この加工データに基づいて2ビット以上の乱数データを提供する加工手段とを備えた物理乱数発生装置である。本発明は、このような手段を設け、直流成分が除去された増幅信号をA/D変換しているため、A/D変換されたデジタル値の各ビットはそのままビット単位の乱数データとして取り扱い可能になっている。したがって、計数ノイズ信号から乱数データを得るのに、多数のノイズ信号を計数する必要がなくなり、1個の乱数を発生させるのに必要な時間を極めて短くすることができる。また、ノイズ源及び乱数発生処理回路を簡素化することができ、ひいては物理乱数発生装置の低価格化にも寄与する。また、一度に2ビット以上の乱数データを得ることができ、より一層多数の乱数データを短時間で提供することができる。さらに、A/D変換手段からのビットデータを微分非直線性を改善する加工手段を用いて加工するようにしているので、たとえ一度に2ビット以上の乱数データを取り出しても十分

に精度の高い乱数を得ることができる。また、請求項2に対応する発明は、請求項1に対応する発明において、A/D変換手段により変換されたデジタル値の平均値を、A/D変換前若しくはA/D変換後のデータに加えるオフセット調整手段を備えた物理乱数発生装置である。本発明は、このような手段を設けたので、請求項1に係る発明と同様な作用効果が得られる他、A/D変換手段からの出力は多くの場合、その頻度分布が正規分布あるいはこれに近い分布に従うと考えられるため、この変換されたデジタル値の平均値をオフセットとして加えることで、より完全に直流成分を除去することができる。さらに、請求項3に対応する発明は、請求項1又は2に対応する発明において、A/D変換手段は6ビット以上の精度を有し、変換されたデジタル値を構成する6ビット以上のビットデータのうち、上位から5ビット目以降の2つ以上のビットデータを取り出して乱数データとする物理乱数発生装置である。本発明は、このような手段を設けたので、請求項1又は2に係る発明と同様な作用効果が得られる。また、A/D変換手段からの出力は多くの場合、その頻度分布が正規分布あるいはこれに近い分布に従うと考えられ、さらにこの場合、後述するシミュレーション結果よれば5ビット目以降のデータのときに確実に一様性が高くなるので、より一層良質な乱数データとすることができる。さらにまた、請求項4に対応する発明は、請求項1〜3に対応する発明において、変換されたデジタル値の頻度分布が平均 N 、分散 σ^2 の正規分布となるとき、変換されたデジタル値が $N \pm \sigma$ 以上の範囲に入る場合のみを有効とする物理乱数発生装置である。本発明は、このような手段を設けたので、請求項1〜3に係る発明と同様な作用効果が得られる他、変換されたデジタル値の有効範囲を $N \pm \sigma$ 以上の範囲とすることで、上位ビットまでその一様性を確実に担保することができ、変換されたデジタル値が多数ビットの場合でも全ビットについて良質な乱数データとして使用することができる。一方、請求項5に対応する発明は、請求項1〜4に対応する発明において、A/D変換手段が出力する2以上の変換されたデジタル値を加算平均する微分非直線性改善手段を備えた物理乱数発生装置である。本発明は、このような手段を設けたので、請求項1〜4に係る発明と同様な作用効果が得られる他、A/D変換手段に由来する微分非直線性を改善して良質な乱数データとすることができる。次に、請求項6に対応する発明は、請求項1〜4に対応する発明において、A/D変換手段の入力値に微分非直線性改善用データをオフセットとして加算するとともに、微分非直線性改善用データに相当する改善用デジタルデータをA/D変換手段の出力値から減算する微分非直線性改善手段を備えた物理乱数発生装置である。本発明は、このような手段を設けたので、請求項1〜4に係る発明と同様な作用効果が得られ

る他、A/D変換手段に由来する微分非直線性を改善して良質な乱数データとすることができる。また、請求項7に対応する発明は、請求項1〜6に対応する発明において、ノイズ源は、熱雑音をノイズ信号として使用する物理乱数発生装置である。本発明は、このような手段を設けたので、請求項1〜6に係る発明と同様な作用効果が得られる他、熱雑音に基づく一様性の高い乱数データを提供することができる。さらに、請求項8に対応する発明は、請求項1〜6に対応する発明において、ノイズ源は、抵抗の熱雑音をノイズ信号として使用する物理乱数発生装置である。本発明は、このような手段を設けたので、抵抗からの熱雑音により請求項8に係る発明と同様な作用効果を得ることができる。さらにまた、請求項9に対応する発明は、請求項1〜6に対応する発明において、ノイズ源は、半導体素子の熱雑音をノイズ信号として使用する物理乱数発生装置である。本発明は、このような手段を設けたので、抵抗からの熱雑音により請求項8に係る発明と同様な作用効果を得ることができる。一方、請求項10に対応する発明は、請求項1〜6に対応する発明において、ノイズ源は、フォトマルチプライヤの光電変換面の熱雑音をノイズ信号として使用する物理乱数発生装置である。本発明は、このような手段を設けたので、抵抗からの熱雑音により請求項8に係る発明と同様な作用効果を得ることができる。次に、請求項11に対応する発明は、請求項1〜6に対応する発明において、ノイズ源は、真空管の陰極より発生する熱雑音をノイズ信号として使用する物理乱数発生装置である。本発明は、このような手段を設けたので、抵抗からの熱雑音により請求項8に係る発明と同様な作用効果を得ることができる。また、請求項12に対応する発明は、請求項1〜6に対応する発明において、ノイズ源は、真空マイクロ素子により発生する電子のゆらぎをノイズ信号として使用する物理乱数発生装置である。本発明は、このような手段を設けたので、請求項1〜6に係る発明と同様な作用効果が得られる他、電子のゆらぎに基づく一様性の高い乱数データを提供することができる。さらに、請求項13に対応する発明は、請求項7〜11に対応する発明において、ノイズ源を高温で一定に保つ恒温手段を備えた物理乱数発生装置である。本発明は、このような手段を設けたので、請求項7〜11に係る発明と同様な作用効果が得られる他、ノイズ源を安定な熱雑音発生状態に保ち、安定なノイズ信号発生により安定した乱数データの提供を行うことができる。さらにまた、請求項14に対応する発明は、請求項1〜13に対応する発明において、乱数データに基づくデータを表示する表示手段を備えた物理乱数発生装置である。本発明は、このような手段を設けたので、請求項1〜13に係る発明による高速で良質な乱数データに基づくデータを表示することを可能とした簡素かつ高性能で低価格な装置を提供することができる。一方、請求項15に対応する発明は、

請求項1～13に対応する発明において、乱数データを用いて信号を変調する信号変調手段を備えた物理乱数発生装置である。本発明は、このような手段を設けたので、請求項1～13に係る発明による高速で良質な乱数データを用いて信号を変調することを可能とした簡素かつ高性能で低価格な装置を提供することができる。次に、請求項16に対応する発明は、請求項1～13に対応する発明において、乱数データを用いてデータの暗号化を行う暗号化手段を備えた物理乱数発生装置である。本発明は、このような手段を設けたので、請求項1～13に係る発明による高速で良質な乱数データを用いてデータの暗号化を行うことを可能とした簡素かつ高性能で低価格な装置を提供することができる。また、請求項17に対応する発明は、請求項1～13記載のうち何れか1項記載の物理乱数発生装置と、物理乱数発生装置からの乱数データをコンピュータに入力可能に構成された、コンピュータのデータ入出力バスとのインターフェイス手段とを備えた物理乱数入力装置である。本発明は、このような手段を設けたので、請求項1～13に係る発明による高速で良質な乱数データをコンピュータに入力することができる。また、この装置の形態として例えば基板形態又はカード形態の装置が考えられる。さらに、請求項18に対応する発明は、請求項1～13記載のうち何れか1項記載の物理乱数発生装置と、物理乱数発生装置からの乱数データをコンピュータの要求に応じてコンピュータ・ネットワークに送出可能に構成された、コンピュータ・ネットワークとのインターフェイス手段とを備えた物理乱数入力装置である。本発明は、このような手段を設けたので、請求項1～13に係る発明による高速で良質な乱数データを、要求に応じネットワークを介してコンピュータに入力することができる。さらにまた、請求項19に対応する発明は、請求項1～13に対応する発明において、生成された乱数データを記録する記憶手段を備え、乱数出力要求があった場合に、この要求に応じて乱数データを供給する物理乱数発生装置である。本発明は、このような手段を設けたので、請求項1～13に係る発明と同様な作用効果が得られる他、要求がないときには生成した乱数を記憶手段に蓄え、要求時にこの蓄えた乱数を出力することで、安定的な乱数の供給を可能とすることができる。一方、請求項20に対応する発明は、請求項1～13記載のうち何れか1項記載の物理乱数発生装置により生成された乱数データを記録した物理乱数記録媒体である。本発明は、このような手段を設けたので、請求項1～13に係る発明による高速で良質な乱数データを記録媒体により提供することができる。次に、請求項21に対応する発明は、請求項20に対応する発明において、記録された乱数データについての検定方法及び又は検定結果を記録した物理乱数記録媒体である。本発明は、このような手段を設けたので、請求項20に係る発明と同様な作用効果が得られる他、

その乱数データに対する信頼性を高めることができる。さらに、請求項22に対応する発明は、ノイズ源からノイズ信号を出力するステップと、ノイズ信号を交流結合により直流分を除去しつつ増幅するAC結合増幅ステップと、AC結合増幅ステップにおいて増幅された増幅ノイズ信号をA/D変換する、2ビット以上の精度を有して2ビット以上のビットデータに変換するA/D変換ステップと、前記A/D変換ステップにより変換された2ビット以上のビットデータを微分非直線性を改善するように加工し、この加工データに基づいて2ビット以上の乱数データを提供するステップとを有する物理乱数発生方法である。本発明は、このような手段を設けたので、請求項1に係る発明と同様な作用効果を得ることができる。さらにまた、請求項23に対応する発明は、請求項1～4に対応する発明において、A/D変換手段の入力信号が変換範囲を超えたときに無効とし、変換範囲を超えずに変換されたデジタル値を乱数データとする物理乱数発生装置である。本発明は、このような手段を設けたので、請求項1～4に係る発明と同様な作用効果を得ることができる他、より良質な乱数データを得ることができる。次に、請求項24に対応する発明は、請求項1～16、19又は23に対応する発明において、加工手段は、補正信号をD/A変換してA/D変換手段への入力前の値に加算し、かつ、補正信号を前記A/D変換手段の出力から差し引くことで乱数データに加工する手段、又は、A/D変換手段から別々に出力されるA/D変換値同士、若しくはA/D変換手段の出力とA/D変換の出力以外のランダムなデータを、加算（排他OR）して乱数データに加工する手段、の何れかである物理乱数発生装置である。

{0014}
{0015}
{0016}
{0017}
{0018}
{0019}
{0020}
{0021}
{0022}
{0023}
{0024}
{0025}
{0026}
{0027}
{0028}
{0029}
{0030}
{0031}
{0032}
{0033}

【0034】
【0035】
【0036】
【0037】
【0038】
【0039】
【0040】
【0041】
【0042】
【0043】
【0044】
【0045】
【0046】
【0047】
【0048】
【0049】
【0050】
【0051】
【0052】
【0053】
【0054】
【0055】
【0056】
【0057】
【0058】
【0059】
【0060】
【0061】
【0062】

【発明の実施の形態】以下、本発明の実施の形態について説明する。

【0063】（発明の第1の実施の形態）図1は本発明の第1の実施の形態に係る物理乱数発生装置の構成例を示すブロック図である。

【0064】この物理乱数発生装置においては、ノイズ源101からのノイズ信号102がAC結合増幅器103に inputs され、その増幅されたノイズ信号104がアナログ・デジタル変換器105にてA/D変換されて乱数データ106として出力されるようになっている。ここで、アナログ・デジタル変換器105は、1ビットあるいは2ビット精度以上のA/D変換器である。

【0065】図2は本実施形態の物理乱数発生装置におけるAC結合増幅器の内部構成例を示す図である。

【0066】AC結合増幅器103は、交流結合により信号の直流成分を通過させないようにしつつ増幅を行う部分であり、ノイズ信号102を入力する入力コンデンサ1801と、入力コンデンサ1801の出力信号を増幅して出力コンデンサに inputs する増幅器1802と、増幅されたノイズ信号104を出力する出力コンデンサ1803とによって構成されている。

【0067】次に、以上のように構成された本発明の実施の形態に係る物理乱数発生装置の動作について説明する。

【0068】まず、ノイズ源101からランダム事象に起因するノイズ成分が出力されるが、そのノイズ信号波形例を図3に示す。

【0069】図3はノイズ信号波形の例を示す図である。

【0070】使用するノイズ源101にもよるが、ノイズ信号波形はオフセット1701電圧（または電流）とその回りに分布するノイズ成分1702の加算合成された波形となる。

【0071】一般的にノイズ源101から得られるノイズ成分のレベルが小さいので、大きな増幅度を有する増幅器を用いてノイズ信号102を増幅する必要がある。しかし、オフセット1701と共に増幅すると増幅器の出力信号が飽和して動作しなくなる。そこで、増幅回路としてAC結合増幅器103が使用され、オフセット1701を除いたノイズ成分1702のみが増幅される。

【0072】すなわち図2に示すAC結合増幅器103では以下のような増幅動作がなされる。

【0073】まず、入力コンデンサ1801により、ノイズ信号102のオフセット1701が除かれ、増幅器1802によりノイズ成分1702のみが増幅される。さらに、出力コンデンサ1803により、増幅器1802自身が有するオフセットを増幅した直流電圧が、増幅されたノイズ信号104に含まれないように除去される。

【0074】したがって、増幅されたノイズ信号104は、AC結合によりオフセットが0で、0の回りにノイズ成分が均等に分布する波形となっている。

【0075】たとえば、増幅されたノイズ信号104を1ビット精度のアナログ・デジタル変換器105を用いてデジタル値に変換すると、増幅されたノイズ信号104の極性に依りて0または1の値となる。ノイズ源から得られる信号はランダムであるから、0または1の値になる順番は確定しない。また、AC結合されているから、0になる確率と1になる確率が等しい。すなわち一様性があり周期性のない質の良い1ビットの乱数データを取得することができる。

【0076】これは、単純なレベルコンパレータを用いて実現できる1ビット乱数データである。さらに2ビット精度以上のアナログ・デジタル変換器105を用いることにより、増幅されたノイズ信号104の頻度分布を有し、周期性のない乱数データを取得することができる。たとえば、ノイズ源101の発生要因が熱雑音であれば、正規分布状の発生確率を有する乱数データを取得することができる。また、アナログ・デジタル変換されたデジタル値を構成する複数のビットの下位のビットから乱数データを作成すれば、増幅されたノイズ源1

04の頻度分布形状に依存しない乱数データを取得することができる。

【0077】更に例えば、12ビットの精度を有するアナログ・デジタル変換器を用いて得られた12ビットの乱数データの中から、下位の2ビットのみを用いると、一様性があり周期性のない2ビットの一様乱数が得られる。

【0078】上述したように、本発明の実施の形態に係る物理乱数発生装置においては、ランダム事象から起因するノイズ源101からノイズ信号102を、AC結合増幅器103を用いてアナログ・デジタル変換器105の変換範囲まで増幅してデジタル値に変換して得られたデジタル・データをもとに乱数データを生成するようにしたので、ノイズ源101の発生確率分布または一様分布で、周期性がない乱数データを得ることができる。

【0079】また、本実施形態の物理乱数発生装置では、ノイズ信号のランダム・パルスを計数するのではなく、増幅されたノイズ信号をアナログ・デジタル変換することにより、1回の変換動作で1つの乱数データを取得することができるため、計数するよりも高速に物理乱数を発生することができる。

【0080】さらに、2ビット以上の精度を有するアナログ・デジタル変換器105を用いる場合には、1回のアナログ・デジタル変換で多ビットの乱数データを発生することができ、ひいては回路構成を簡素化することができる。

【0081】（発明の第2の実施の形態）第1の実施形態では、ランダム・ノイズ源から得られるノイズ信号をアナログ・デジタル変換器を用いてデジタル・データに変換したときの頻度分布は正規分布となる。この場合、平均値の回りに一様に偶数または奇数データが分布することになり、変換されたデジタル値を構成するすべてのビットの奇数・偶数の頻度分布は一様になる。

【0082】しかし、増幅回路やアナログ・デジタル変換器のオフセットの絶対値の存在、またはオフセットのドリフトにより、一様性が崩れる可能性がある。これに対し、本実施形態では、これらをキャンセルするオフセットを加えることにより、奇数・偶数の頻度分布が常に一様になるようにし、一様性が保証された物理乱数を発生するものである。

【0083】図4は本発明の第2の実施の形態に係る物理乱数発生装置の構成例を示すブロック図であり、図1と同一部分には同一符号を付してその説明を省略する。

【0084】この物理乱数発生装置は、第1の実施形態と同様に構成される他、アナログ・デジタル変換器105からの出力206をもとにオフセット調整信号202出力するオフセット検出器201と、この信号202をD/A変換して出力するデジタル・アナログ変換器203と、アナログ・オフセット調整信号204に変換

し、増幅されたノイズ信号104から引き去る演算器207とを備え、アナログ信号によるオフセット調整機能を有している。

【0085】次に、以上のように構成された本発明の実施の形態に係る物理乱数発生装置の作用について説明する。

【0086】第1の実施形態で説明したように、AC結合増幅器103を用いることにより、増幅されたノイズ信号104のオフセット成分（直流成分）が小さくなる。しかし、この成分がアナログ・デジタル変換器105自身のオフセット成分と同じ値にならない限り、頻度分布の平均値が0にはならない。すなわちオフセット成分の存在により、アナログ・デジタル変換器のMSBが0になる確率と1になる確率とが変わるため一様性に誤差が生じるのである。

【0087】また、微小な他のノイズ成分により正規分布からのずれが発生することも予想される。そこで、正規分布の平均値とアナログ・デジタル変換器105自身のオフセットが一致するように調整することにより、乱数データの一様性を向上させるのである。

【0088】また、オフセットや正規分布からのずれが微小であり、温度等の環境条件により変化する可能性もあるため、これらの調整を自動的におこなう必要がある。本実施形態ではこの自動調整方法としてはアナログ方式を採用し、この自動調整機能部分が以下のように動作する。

【0089】まず、オフセット検出器201により、アナログ・デジタル変換器105に変換されたデジタル値206からその平均値が求められ、これにより増幅されたノイズ信号104とアナログ・デジタル変換器105との間のオフセット量が検出される。

【0090】オフセット検出器201からは検出されたオフセット量に基づきデジタル・オフセット調整信号202が出力される。

【0091】次に、デジタル・オフセット調整信号202がデジタル・アナログ変換器203によりD/A変換されアナログ・オフセット調整信号204として出力される。

【0092】アナログ・オフセット調整信号204は、演算器207に入力され、ここで増幅されたノイズ信号104から当該調整信号204が引き去られ、これによりオフセット量が自動的に零に調整される。

【0093】上述したように、本発明の実施の形態に係る物理乱数発生装置は、第1の実施形態と同様な構成を設けた他、オフセット検出器201、デジタル・アナログ変換器203及び演算器207からなるオフセット自動調整機能を設けたので、第1の実施形態と同様な効果が得られる他、増幅回路やアナログ・デジタル変換器等の種々のオフセットやオフセットドリフト等をキャンセルして奇数・偶数の頻度分布が常に一様になる、一

様性が保証された物理乱数を発生させることができる。

【0094】（発明の第3の実施の形態）本実施形態では、第2の実施形態と同様なオフセット自動調整機能をデジタル的に実現させるものである。

【0095】図5は本発明の第3の実施の形態に係る物理乱数発生装置の構成例を示すブロック図であり、図1及び図2と同一部分には同一符号を付してその説明を省略する。

【0096】この物理乱数発生装置は、第1の実施形態と同様に構成される他、第2の実施形態と同様なオフセット検出器201と、オフセット検出器201からのデジタル・オフセット調整信号202をアナログ・デジタル変換器105からの出力206に加算し乱数データとして出力するデジタル加算器205を備え、デジタル信号によるオフセット調整機能を有している。

【0097】以上のように構成された本発明の実施の形態に係る物理乱数発生装置においては、アナログ信号によるオフセット調整の場合と同様に、オフセット検出器201からデジタル・オフセット調整信号202が出力される。この調整信号202がアナログ・デジタル変換器105からの変換されたデジタル値206とデジタル加算器205により加算され、オフセット量が自動調整される。

【0098】上述したように、本発明の実施の形態に係る物理乱数発生装置は、第1の実施形態と同様な構成を設けた他、オフセット検出器201及びデジタル加算器205からなるオフセット自動調整機能を設けたので、第1及び第2の実施形態と同様な効果が得られる。他、第2の実施形態のようにアナログ回路を使用することによる部品点数の増加やオフセット印加回路自身のオフセット電圧変動要素を持ち込みを防止することができる。

【0099】また、オフセット自動調整機能でもデジタル処理が行われるので、温度特性に依存することもない。さらに、デジタル回路は容易にLSI化等の小型化を実現することができ、小形化に際し有利である。

【0100】（発明の第4の実施の形態）第1の実施形態の物理乱数発生装置において、オフセットの調整をせずにアナログ・デジタル変換をおこなったとき、増幅器やアナログ・デジタル変換器のオフセット・ドリフトやゲイン変動、またはノイズ源のノイズ・レベル変動があつた場合、アナログ・デジタル変換器の上位ビットが特に大きく影響を受けることになる。

【0101】シミュレーションによれば、多少のドリフトや変動があつた場合でも一様性を保つことができるのは、5ビット目以降のビット・データである。

【0102】そこで、本実施形態では、6ビット精度以上のアナログ・デジタル変換器を使用し、上位から5ビット目以降の2つ以上のビット・データを乱数データとすることにより、各ビットの偶数・奇数発生頻度の一

様性を保つ乱数データを発生させるものである。

【0103】図6は本発明の第4の実施の形態に係る物理乱数発生装置の構成例を示すブロック図であり、図1と同一部分には同一符号を付してその説明を省略する。

【0104】物理乱数発生装置は、第1の実施形態の装置において、アナログ・デジタル変換器105として6ビット精度以上のA/D変換器が使用されるとともに、その変換されたデジタル206を構成するビットのうち、上位(MSB: Most Significant Bit)から5番目以降のビットを乱数データ301として取り出すように構成されている。

【0105】次に、以上のように構成された本発明の実施の形態に係る物理乱数発生装置の作用について説明する。

【0106】図7はオフセット及びゲイン変動に対する一様性に関するシミュレーション結果を示す図である。

【0107】まず、図7(a)には、オフセットの変動に対する一様性の変化が示めされている。同図に示すように、オフセットをアナログ・デジタル変換器105の変換範囲に対して $\pm 10\%$ 程度変化させ、変換されたデジタル値206を構成する各ビット毎に、0または1になる頻度を調べると、上位ビットほどオフセットに対する一様性のずれが大きい結果となる。

【0108】一方、図7(b)には、ゲインの変動に対する一様性の変化が示めされている。増幅されたノイズ信号104を標準正規分布とし、ゲインを変化させ、アナログ・デジタル変換器105の変換範囲を $\pm 6\sigma \sim \pm \sigma$ とする。このとき、変換されたデジタル値206を構成する各ビット毎に、0または1になる頻度を調べると、同図に示すように、上位ビットほどゲイン変動に対する一様性のずれが大きい結果となる。

【0109】本実施形態の装置は、以上の知見に基づき、変換されたデジタル値206のうち上位から5ビット目以降のデータが乱数データ301として取り出される。

【0110】上述したように、本発明の実施の形態に係る物理乱数発生装置は、第1の実施形態と同様な構成を設けた他、上位(MSB)側から数えて第5ビット以降のビットを乱数データ301として採用するようにしたので、第1の実施形態と同様な効果が得られる他、より一層、一様性の良い乱数データを得ることができる。

【0111】（発明の第5の実施の形態）本実施形態は、各ビットの偶数・奇数発生頻度の一様性に関するシミュレーション結果に基づき、ノイズ源のノイズ分布に対しアナログ・デジタル変換器の変換範囲を明確にすることにより、各ビットの偶数・奇数発生頻度の一様性を保つ手法を与えるものである。

【0112】図8は本発明の第5の実施の形態に係る物理乱数発生装置におけるA/D変換範囲を決定するためのシミュレーション結果を示す図である。なお、本実施

形態は、図1に示す第1の実施形態と同様な構成を有する物理乱数発生装置に適用される。

【0113】図8には、変換されたデジタル値206の頻度分布と本実施形態のアナログ・デジタル変換器の変換値の関係が示されている。同図において、 $N \pm \sigma$ 以上のアナログ・デジタル変換器105の変換範囲401の両側に、オーバーフロー範囲402とアンダーフロー範囲403が存在しており、これらの範囲402及び403は、すなわちオーバーレンジ範囲404である。

【0114】本実施形態の物理乱数発生装置は、このようにアナログ・デジタル変換器105の変換範囲401が設定され、第4の実施形態と同様に変換されたデジタル値206の5ビット目以降を乱数データに用いる他、第1の実施形態と同様に構成されている。

【0115】ここで、ゲインを大きくするということは、頻度分布に対する変換範囲を狭くすることに対応する。ゲインを大きくすると、相対的に平均値付近の変化が少なくなるとみなせるので、オフセットの変動に対する一様性の変化が小さくなり、上位ビットを乱数データとして採用できるようになる。

【0116】しかし、増幅されたノイズ信号104（図1）がアナログ・デジタル変換器105の変換範囲を越える確率が高くなるため、乱数発生効率が低下する。低下の度合いは、変換されたデジタル値206の確率分布に従い、正規分布の場合、アナログ・デジタル変換器105の変換範囲が、増幅されたノイズ信号104に対して $N \pm \sigma$ のとき約30%の損失が生じる。

【0117】したがって、変換範囲が $N \pm \sigma$ よりも大きい範囲となるようゲインを下げ、ゲインを下げることによって生じる上位（MSB側）ビットの一様性の低下（図7（b）参照）については、変換されたデジタル値206の一様性の低下していない5ビット目以降を用いることで対応する。

【0118】上述したように、本発明の実施の形態に係る物理乱数発生装置は、第1及び第4の実施形態と同様な構成を設けた他、ノイズ源のノイズ分布に対するアナログ・デジタル変換器105の変換範囲401を $N \pm \sigma$ 以上としたので、第1及び第4の実施形態と同様な効果が得られる他、各ビットの偶数・奇数発生頻度の一様性を一層確実に保つことができる。

【0119】（発明の第6の実施の形態）本実施形態は、第5の実施形態と同様にアナログ・デジタル変換器の変換範囲401（図8）を予め規定することにより一様性の高い乱数を得ようとするものである。つまり、ノイズ信号がアナログ・デジタル変換器の変換範囲を越えたときの具体的な取扱いに関する実施形態を示すものである。

【0120】変換範囲401を越えたときには、アナログ・デジタル変換器から出力されるデジタル・デー

タの値は保証されない。この場合、変換範囲を越えたときに出力されるデータを構成するビット・パターンが固定化される可能性があり、多ビット・データを乱数データとした時に著しくビット間の相関に影響を与える。

【0121】そこで、本実施形態では、変換範囲401を越えたときに出力されるデータはランダム性をもたないものとみなし、乱数発生から除外するものである。

【0122】図9は本発明の第6の実施の形態に係る物理乱数発生装置の構成例を示すブロック図であり、図1と同一部分には同一符号を付してその説明を省略する。

【0123】この物理乱数発生装置は、アナログ・デジタル変換器105からの変換後のデジタル値501及びオーバーレンジ信号503に基づき、変換範囲401内のデジタル値501のみを乱数データ106として出力するオーバーレンジ処理器502が設けられる他、第1の実施形態と同様に構成されている。

【0124】このように構成された物理乱数発生装置においては、まず、増幅されたノイズ信号104がアナログ・デジタル変換器105の変換範囲を越えた場合には、当該A/D変換器105からオーバーレンジ信号503が発生するようになっている。

【0125】このオーバーレンジ信号503を受けたオーバーレンジ処理器502により、アナログ・デジタル変換後のデジタル値501が処理され、オーバーレンジ範囲404にあるデジタル値501が乱数データ106から取り除かれる。ここで、オーバーレンジ処理器502の具体的な処理内容は、乱数データ106の出力速度により異なることになる。

【0126】例えば乱数データ106を一定の速度で出力する必要がある場合は、オーバーレンジ処理器502にはFIFOメモリのような緩衝器を内蔵し、オーバーレンジ処理によって生じるデータ出力の欠落がないように乱数データ106が出力される。

【0127】この場合、乱数データ出力速度は、アナログ・デジタル変換器105のデータ変換速度より遅くなる。遅くなる割合は、増幅されたノイズ信号104をアナログ・デジタル変換したときの頻度分布で決まる。

【0128】乱数データを一定の速度で出力する必要がない場合、たとえば、乱数データ106の入出力においてハンドシェイクが行われる場合は、有効な乱数データを得るまでデータ出力を保留する。

【0129】上述したように、本発明の実施の形態に係る物理乱数発生装置は、第1の実施形態と同様な構成を設けた他、オーバーレンジ処理器502により変換範囲のデジタル値501のみを乱数データ106として出力するようにしたので、第1の実施形態と同様な効果が得られる他、各ビットの偶数・奇数発生頻度の一様性を一層確実に保つことができる。つまり、変換範囲を越えたときに出力されるデータはランダム性をもたないもの

とみなし、乱数発生から除外することにより、発生した乱数の性質を向上させることができる。

【0130】（発明の第7の実施の形態）本実施形態では、アナログ・デジタル変換器の変換範囲について種々の位置で変換動作を行うことにより、微分非直線性による一様性の低下を改善するものである。

【0131】高速なアナログ・デジタル変換器の微分非直線性は、最悪 $\pm 0.5 \text{ LSB}$ である。たとえば、10ビット精度のA/D変換器は1.024Vの電圧を1024に分割してデジタル値とすることができるが、微分非直線性の影響により、変換結果がNとN+1との間の電圧は正確に1mV（1.024/1024）にはならない。変換結果Nに応じて0.5mVから1.5mVの値となる。これは、アナログ・デジタル変換結果を乱数データとして用いる場合の一様性の低下につながる。

【0132】そこで、本発明では、微分非直線性が変換結果Nに依存していることを利用し、アナログ信号に既知の電圧を加え、アナログ・デジタル変換を行ない、アナログ信号に加えた値と同じ値のデジタル値を引き去る機構を物理乱数発生装置に加えるものである。

【0133】図10は本発明の第7の実施の形態に係る物理乱数発生装置の主要部の構成例を示すブロック図である。

【0134】この物理乱数発生装置は、アナログ・デジタル変換器105の入力にアナログ補正信号2104を加え、変換器105の出力からデジタル補正信号2102を差し引くように構成される他、第1～第6の実施形態何れかと同様に構成されている。このために物理乱数発生装置には、補正信号発生器2101と、デジタル・アナログ変換器2103と、加算器2106と、デジタル減算器2105とが設けられている。

【0135】このように構成された物理乱数発生装置においては、まず、補正信号発生器2101よりデジタル補正信号2102が発生する。このデジタル補正信号2102は、デジタル・アナログ変換器2103によりアナログ補正信号2104に変換され、増幅されたノイズ信号104と加算される。この加算値により、アナログ・デジタル変換器105により変換されたデジタル値206が得られる。

【0136】一方、デジタル補正信号2102は、デジタル減算器2105に入力され、変換されたデジタル値206から値を引き去ることにより乱数データ106が得られる。

【0137】上述したように、本発明の実施の形態に係る物理乱数発生装置においては、アナログ信号に既知の電圧を加え、アナログ・デジタル変換を行い、アナログ信号に加えた値と同じ値のデジタル値を引き去るようにしたので、第1～第6の実施形態と同様な効果が得られる他、アナログ・デジタル変換器105の変換結果Nの値を変えながら、乱数データ106としては同じ

値を得ることができ、変換結果Nに依存した微分非直線性が平均化され、乱数の一様性を改善することができる。

【0138】（発明の第8の実施の形態）本実施形態は、第7の実施形態と同様に、アナログ・デジタル変換器の微分非直線性による一様性の低下を改善するものである。すなわち本実施形態における微分非直線性の影響を低減する基本的な原理は第7の実施形態と同様であり、同じアナログ電圧をデジタル値に変換する場合、異なる値を発生させることにより、変換結果Nに依存した一様性の低下を改善するものである。

【0139】図11は本発明の第8の実施の形態に係る物理乱数発生装置の主要部の構成例を示すブロック図である。

【0140】この物理乱数発生装置は、アナログ・デジタル変換器105の出力を格納するレジスタ（#1）2201及びレジスタ（#2）2202と、両レジスタ2201、2201の値を加算するデジタル加算器2203が設けられる他、第1～第6の実施形態何れかと同様に構成されている。

【0141】このように構成された物理乱数発生装置においては、まず、アナログ・デジタル変換器105により変換されたデジタル値206がレジスタ2201及びレジスタ2202に交互に記録される。

【0142】次に、レジスタ2201及びレジスタ2202の出力のデジタル加算器2203により加算平均が求められ、乱数データ106として出力される。

【0143】上述したように、本発明の実施の形態に係る物理乱数発生装置においては、交互に変換されたデジタル値206により加算平均を求めて乱数データ106として用いるようにしたので、第1～第6の実施形態と同様な効果が得られる他、変換結果Nに依存した乱数一様性の低下を改善し、微分非直線性の影響を低減させることができる。

【0144】これにより、アナログ・デジタル変換されたデジタル値をデータの加算によりビットが1又は0になる確率を一様にするすることができる。すなわち加算する相手をランダムな値とすることにより、ランダム性を失うことなく微分非直線性を改善することができる。

【0145】なお、図11に示す構成の物理乱数発生装置では、乱数データ106の発生頻度がアナログ・デジタル変換器105の変換頻度の半分になってしまう。

【0146】そこで、乱数データ106の発生頻度を低下させない方法としては、例えばレジスタ2202に入力する値を、もう1系統のノイズ源を用いてデジタル値に変換された値を用いてもよい。また、乱数データとして多ビットを用いるのであれば、周期的なデジタル値をレジスタ#2に接続して加算（排他OR）することによつて、一様性を向上することもできる。

【0147】（発明の第9の実施の形態）本実施形態で

は、上記第1～第8の実施形態に使用され得るノイズ源として、アナログ・デジタル変換した場合の頻度分布が正規分布に従うノイズ源について説明する。本実施形態は熱雑音を利用するものであり、熱雑音は統計的事象から引き起こされ、熱雑音のゆらぎは正規分布になる。

【0148】図12は本発明の第9の実施の形態に係る物理乱数発生装置におけるノイズ源の一例を示す構成図である。なお、このノイズ源101は、第1～第8の実施形態に示す物理乱数発生装置に適用されるものである。

【0149】このノイズ源101は抵抗の熱雑音を利用するものであり、ノイズ源101においては電源Vから抵抗601と抵抗602とが直列接続され接地され、同様に電源Vからヒータ603とヒータ604とが直列接続され接地されている。また、このヒータ603及びヒータ604は、それぞれ抵抗601及び抵抗602を加熱するように配置され、抵抗601と抵抗602との間からノイズ信号102が出力されるようになっている。

【0150】抵抗の熱雑音は小さいため、ヒータ603およびヒータ604により抵抗を加熱し、熱雑音を大きくするとともに、抵抗601および抵抗602の温度を一定とすることにより、安定したノイズ信号102が得られる。

【0151】上述したように、本発明の実施の形態に係る物理乱数発生装置においては、上記したノイズ源を用いるようにしたので、安定したノイズ信号により偶数・奇数発生頻度の一様性の高い乱数データを得ることができる。

【0152】（発明の第10の実施の形態）本実施形態では、第9の実施形態と同様に、上記第1～第8の実施形態に使用され得るノイズ源について説明するものである。本実施形態においても熱雑音を利用される。

【0153】図13は本発明の第10の実施の形態に係る物理乱数発生装置におけるノイズ源の一例を示す構成図である。なお、このノイズ源101は、第1～第8の実施形態に示す物理乱数発生装置に適用されるものである。

【0154】このノイズ源101は、トランジスタを使用するものであり、電源接地間に直列接続された抵抗701及び抵抗702との間からトランジスタ703に接続している。これによりトランジスタ703にバイアスが掛けられる一方、電源接地間に抵抗704、トランジスタ703及び抵抗707が直列接続されている。そして、抵抗704の両端に発生するトランジスタ703の熱雑音を利用し、抵抗704、トランジスタ703間からノイズ信号102が出力されるようになっている。

【0155】上述したように、本発明の実施の形態に係る物理乱数発生装置においては、上記したノイズ源を用いるようにしたので、安定したノイズ信号により偶数・

奇数発生頻度の一様性の高い乱数データを得ることができる。

【0156】（発明の第11の実施の形態）本実施形態では、第9の実施形態と同様に、上記第1～第8の実施形態に使用され得るノイズ源について説明するものである。本実施形態においても熱雑音を利用される。

【0157】図14は本発明の第11の実施の形態に係る物理乱数発生装置におけるノイズ源の一例を示す構成図である。なお、このノイズ源101は、第1～第8の実施形態に示す物理乱数発生装置に適用されるものである。

【0158】このノイズ源101は、ツェナーダイオードを使用する場合であり、電源接地間に抵抗705とツェナーダイオード706が接続され、この両者間からノイズ信号102が出力されるようになっている。

【0159】このようにツェナーダイオードを用いる場合には、抵抗705によりツェナーダイオード706にツェナー電流を流し、抵抗705の両端に発生する熱雑音を利用する。ツェナーダイオード706に電流を流す回路としては、抵抗ではなく例えば定電流回路でも良い。

【0160】上述したように、本発明の実施の形態に係る物理乱数発生装置においては、上記したノイズ源を用いるようにしたので、安定したノイズ信号により偶数・奇数発生頻度の一様性の高い乱数データを得ることができる。

【0161】（発明の第12の実施の形態）本実施形態では、第9の実施形態と同様に、上記第1～第8の実施形態に使用され得るノイズ源について説明するものである。本実施形態においても熱雑音を利用される。

【0162】図15は本発明の第12の実施の形態に係る物理乱数発生装置におけるノイズ源の一例を示す構成図である。なお、このノイズ源101は、第1～第8の実施形態に示す物理乱数発生装置に適用されるものである。

【0163】このノイズ源101は、フォトマルチプライヤを利用するものであり、同図に示すように、フォトマルチプライヤ801、バイアス印加用の抵抗806、807及び808並びに高圧電源809より構成される。

【0164】フォトマルチプライヤ801は、光を電子に変換して増幅する。

【0165】すなわちフォトマルチプライヤ801の光電面802に光が当たると、そこから電子が発生する。発生した電子は電位の高い電極803に衝突し、電極803への電子衝突によりさらに多数の電子が発生する。この発生した電子は、さらに電位の高い電極804に衝突する。

【0166】このような電子の増倍を繰り返し、最後の電極805に電子が衝突する。ここまでに到達した電子

の数から光電面に入射した非常に微弱な光の量を知ることができ、ここよりノイズ信号102が得られる。

【0167】ところで、光電面802を遮光した場合でも、光電面に存在する熱電子によりフォトマルチプライヤの出力にはノイズ信号102が発生する。通常、このようにして発生するノイズを暗電流と呼び、光の量を測定するときの下限となるため小さい方が良いとされるが、熱雑音に起因したノイズであるため物理乱数のノイズ源として利用できる。

【0168】上述したように、本発明の実施の形態に係る物理乱数発生装置においては、上記したノイズ源を用いるようにしたので、安定したノイズ信号により偶数・奇数発生頻度の一様性の高い乱数データを得ることができる。

【0169】（発明の第13の実施の形態）本実施形態では、第9の実施形態と同様に、上記第1～第8の実施形態に使用され得るノイズ源について説明するものである。本実施形態においても熱雑音が利用される。

【0170】図16は本発明の第13の実施の形態に係る物理乱数発生装置におけるノイズ源の一例を示す構成図である。なお、このノイズ源101は、第1～第8の実施形態に示す物理乱数発生装置に適用されるものである。

【0171】このノイズ源101は、真空管を利用するものであり、高圧電源906がバイアス印加用の抵抗905を介して2極真空管901に接続され、この2極真空管901にはさらにヒータ電源907が接続されて構成されている。

【0172】2極真空管901においては、ヒータ902を用いて電極903を加熱することにより熱電子が発生し、発生した電子は電位の高い電極904に到達する。電極903から電極904に流れた電子の量は、抵抗905の両端電圧を測定することにより得られる。

【0173】得られた電流値は、熱雑音を起因とするゆらぎを有し、このゆらぎをノイズ信号102として使用する。なお、ここで使用するヒータ電源907にはACノイズの影響が出ないよう直流電源を用いることが望ましい。

【0174】上述したように、本発明の実施の形態に係る物理乱数発生装置においては、上記したノイズ源を用いるようにしたので、安定したノイズ信号により偶数・奇数発生頻度の一様性の高い乱数データを得ることができる。

【0175】（発明の第14の実施の形態）本実施形態では、第9の実施形態と同様に、上記第1～第8の実施形態に使用され得るノイズ源について説明するものである。本実施形態においても熱雑音が利用される。

【0176】図17は本発明の第14の実施の形態に係る物理乱数発生装置におけるノイズ源の一例を示す構成図である。なお、このノイズ源101は、第1～第8の

実施形態に示す物理乱数発生装置に適用されるものである。

【0177】このノイズ源101は、真空マイクロ素子を利用するものであり、高圧電源1006がバイアス印加用の抵抗1005を介して真空マイクロ素子1001に接続され、この真空マイクロ素子1001には制御電源1007が接続されて構成されている。

【0178】接地された電極1002の近傍に電極1003をおき、この電極1003に制御電源1007より電場をかけると、トンネル効果により電極1002から電子が発生する。発生した電子は電極1003に向って移動するが、電極1002と電極1003を挟むように配置される、より高い電位の電極1004に引きつけられる。このようにして、電極1002と電極1004との間に電流が流れ、流れた電流は抵抗1005の両端電圧として観測される。得られた電流値は統計的に発生するトンネル効果を起因とするゆらぎを有し、このゆらぎをノイズ信号102として使用する。

【0179】上述したように、本発明の実施の形態に係る物理乱数発生装置においては、上記したノイズ源を用いるようにしたので、安定したノイズ信号により偶数・奇数発生頻度の一様性の高い乱数データを得ることができる。

【0180】（発明の第15の実施の形態）本実施形態は、第9～第13の実施形態のノイズ源に適用されるものであって、ノイズ源からのノイズ信号を安定化させるためのものである。

【0181】すなわち、熱雑音は絶対温度の平方根に比例して変動することから、ノイズ源から発生する信号レベルが周囲温度の影響により変動するので、これを防止するものである。

【0182】なお、第14の実施形態に示す真空マイクロ素子のゆらぎ成分は、トンネル効果によるものであり、温度の影響を受けないためこの方法による定温化の効果が得られないことから除外している。

【0183】図18は本発明の第15の実施の形態に係る物理乱数発生装置におけるノイズ源恒温化装置の一例を示す構成図である。

【0184】このノイズ源恒温化装置では、ノイズ源素子2001を恒温ケース2002に収納する。恒温ケース2002には、ヒータ2003が内蔵されており、恒温制御器2005により温度が一定になるよう制御されている。なお、ノイズ源素子2001は、第7～第12の実施形態のノイズ源101に使用されるノイズ源の素子部分である。

【0185】ノイズ源素子2001の温度は、測温体2004を用いて測定し、温度信号2006として恒温制御器2005に接続される。恒温制御器2005は、温度信号2006にもとづきヒータ加熱信号2007を制御し、ノイズ源素子2001の温度が一定になるようヒ

ータ加熱電力を制御する。

【0186】一定に制御する温度としては、ノイズ源素子2001の動作限界よりも低く、環境温度よりも高い温度を選択する。たとえば、コンピュータ周囲温度を25℃、物理乱数発生装置の周辺温度を35℃、ノイズ源素子2001の上限動作温度を55℃とし、コンピュータ周辺温度が空調により±5℃変化して物理乱数発生装置の周辺温度が最高40℃まで上昇すると仮定した場合、制御する温度の値を45℃～50℃にすれば、冷却機能を内蔵せずにノイズ源素子2001の温度をヒータ2003だけで一定に制御することができる。

【0187】上述したように、本発明の実施の形態に係る物理乱数発生装置においては、そのノイズ源101をノイズ源恒温化装置により温度を一定に保つようにしたので、ノイズレベルの変動を防ぐとともに、高温で一定に保つことにより、熱雑音が出やすくなり、さらに冷却を不要とすることができる。

【0188】（発明の第16の実施の形態）本実施形態から第23の実施形態までは第1～第15の実施形態で説明した物理乱数発生装置を利用した装置について説明する。

【0189】図19は本発明の第16の実施の形態に係る物理乱数発生装置を用いた表示装置の構成例を示すブロック図である。

【0190】この表示装置は、物理乱数発生回路100からの乱数データ106が表示処理器1101に入力され、さらにこの表示処理器1101からの表示データ1102が表示器1103に表示されるようになってい

る。

【0191】表示処理器1101は、制御パネル1104の制御により、入力された乱数データ106を利用して入力し表示データ1102を出力する。

【0192】制御パネル1104には、ボタン等が付いており、ボタンを押した結果が制御信号1105として表示処理器1101に入力されるようになっている。

【0193】物理乱数発生回路100は、第1～第15の実施形態で説明した物理乱数発生装置の何れかと同様に構成されている。

【0194】なお、この物理乱数発生回路100及び表示処理器1101からなる乱数出力部分には、種々の乱数発生機能が組み込まれている。この種々の乱数発生機能は、例えばアナログ・ディジタル変換器105のビット数を変更することで発生させる一様乱数データ106の値の範囲を変更し、表示処理器1101にて受信した乱数データ106の取捨選択をするものである。

【0195】このように構成された物理乱数発生装置を用いた表示装置の動作について説明する。

【0196】たとえば、サイコロの目を乱数で出す場合を考える。まず、制御パネル1104のボタンで乱数発生機能をサイコロモードに切り替える。

【0197】ここで3ビットの一様乱数データ106を用いて0から7の値を発生するが、サイコロには1から6の目しかないので、0または7が出たときは、1から6の目が出るまで乱数を発生するようにしておく。

【0198】制御パネル1104のボタンを押して乱数の発生を開始する。乱数の発生を開始したことが分かるように発生した乱数の値を表示器1103に表示する。次にボタンを押して乱数の発生を停止し、そのときの乱数の値を表示器1103に表示する。

【0199】次に、ビンゴゲームの数字を出す場合を考える。まず、制御パネル1104のボタンで乱数発生機能をビンゴモードに切り替える。発生させた乱数データのうち、ビンゴゲームに必要な数値が出たときの処理はサイコロのときと同じであるが、ビンゴゲームの場合は値は1度しか発生しないため、1度発生した値を覚えておく必要がある。さらに、ゲームが終了したら、1度発生した値をすべて消去する機能も必要であるから、ビンゴモードのスタート、ストップ機能のボタンに加えてリセット機能を有するボタンも必要である。

【0200】上述したように、本発明の実施の形態に係る物理乱数発生装置を用いた表示装置においては、物理乱数発生回路100、表示処理器1101及び制御パネル1104を設けたので、手軽に乱数を取得し、種々の用途に応用することができる。たとえば乱数表の作成、さいころの模擬、ビンゴゲームの数字発生、福引き抽選機等の用途に使用できる。このような用途に適用することで、ノイズ源および乱数データ発生回路の大量生産が可能になり、装置の小型化、低価格化を実現させることができる。

【0201】（発明の第17の実施の形態）本実施形態では、物理乱数発生装置を用いた通信装置について説明する。このような通信方法として例えばスペクトラム拡散方式があり、物理乱数発生装置で発生した乱数データを用いて周波数変調を行なうことにより、第三者に知られることなく通信することができる。このような用途の乱数には、乱数に周期性がないことと、一様性が求められる。疑似乱数は周期性があり一様性も完全ではないので、乱数としては物理乱数を用いるほうが適している。

【0202】図20は本発明の第17の実施の形態に係る物理乱数発生装置を用いた通信装置の構成例を示すブロック図である。

【0203】この通信装置は、物理乱数発生回路100、変調信号発生器1201及び変調器1203により構成されている。なお、物理乱数発生回路100は、第1～第15の実施形態で説明した物理乱数発生装置の何れかと同様に構成されている。

【0204】このように構成された物理乱数発生装置を用いた通信装置は以下のように動作する。

【0205】まず、物理乱数発生回路100からの乱数データ106をもとに変調信号発生器1201におい

て、変調信号1202が生成される。そして、送信データ1204と変調信号1202が変調器1203により変調され、送信信号1205が作成され送信される。

【0206】スペクトラム拡散方式の通信方式では、このように乱数データから変調信号を作成している。データ通信の場合は、第3者に変調信号を知られてはならないが、通信をおこなう者同士は変調信号を互いに知っておく必要がある。

【0207】そこで、変調信号発生器1201の役割は、乱数データ106から変調信号を作成し、新たな変調信号を通信を行う者同士で認識されるまで保持し、認識された時点で新しい変調信号に更新することにある。

【0208】上述したように、本発明の実施の形態に係る物理乱数発生装置を用いた表示装置においては、スペクトラム拡散方式の通信等に物理乱数発生回路100からの物理乱数データ106を使用するようにしたので、装置の小型化、低価格化を実現させることができるとともに、通信の秘匿性を確実に確保することができる。

【0209】すなわち疑似乱数のように、一定のルールで作成された変調信号の場合、一旦変調信号を解読すると新たな変調信号を発生しても容易に推定されるという問題があるが、物理乱数の場合は周期性や発生する順番に関するルールがないため、一度解読されても容易に類推することができない。

【0210】（発明の第18の実施の形態）本実施形態では、物理乱数発生器を用いたデータ暗号化装置について説明する。たとえば、ABCという文字を暗号化して他の3文字に置き換えるために乱数データを用いる。また、戦闘機において、互いに見方であることを示す識別コードとして暗号が使用されている。このような暗号は頻繁に変更し、第3者に容易に解読されない必要がある。

【0211】図21は本発明の第18の実施の形態に係る物理乱数発生装置を用いたデータ暗号化装置の構成例を示すブロック図である。

【0212】このデータ暗号化装置は、物理乱数発生回路100、暗号化装置1302により構成されている。なお、物理乱数発生回路100は、第1～第15の実施形態で説明した物理乱数発生装置の何れかと同様に構成されている。

【0213】このように構成された物理乱数発生装置を用いたデータ暗号化装置は以下のように動作する。

【0214】元データ1301とともに物理乱数発生回路100からの乱数データ106が暗号化装置1302に入力される。暗号化装置1302においては、この元データ1301及び乱数データ106によって、暗号化データ1303が作成され出力される。

【0215】上述したように、本発明の実施の形態に係る物理乱数発生装置を用いた表示装置においては、暗号化に物理乱数発生回路100からの乱数データ106を

利用するようにしたので、装置の小型化、低価格化を実現させることができるとともに、暗号化するコードとして物理乱数データ106を使用することにより、周期性、データ発生の順番などの問題をなくすことができ、暗号化の秘匿性を向上させることができる。

【0216】なお、従来のように、この乱数として疑似乱数を使用する場合、周期性や一様性に関する課題がある。すなわち良く知られている疑似乱数発生手法を用いて発生された乱数データについては、研究され尽くされており、乱数系列の一部から乱数系列全体を推定することも可能になっているため、疑似乱数では完全な秘匿性を確保できない可能性がある。これに対し、物理乱数発生装置から得られる乱数データは、周期性がなく、一様性が保証された良質の乱数であるため、秘匿性を確保することができる。

【0217】（発明の第19の実施の形態）本実施形態では、発生した物理乱数データを計算機に取り込むことを可能にする乱数入力装置について説明する。

【0218】図22は本発明の第19の実施の形態に係る物理乱数発生装置を用いた乱数入力装置の一構成例を示すブロック図である。

【0219】図23は本発明の第19の実施の形態に係る物理乱数発生装置を用いた乱数入力装置の他の構成例を示すブロック図である。

【0220】図24は本発明の第19の実施の形態に係る物理乱数発生装置を用いた乱数入力装置のさらに他の構成例を示すブロック図であり、図19～図21において同一部分には同一符号を付している。

【0221】図22～図24に示す乱数入力装置においては、物理乱数発生回路100から出力された乱数データ106がバス・インタフェース1401に入力され、さらにバス・インタフェース1401からバスインタフェース信号1402に変換された乱数が計算機に対して出力されるようになっている。

【0222】なお、物理乱数発生回路100は、第1～第15の実施形態で説明した物理乱数発生装置の何れかと同様に構成されている。

【0223】バスインタフェース信号1402は、コンピュータ・データ入出力バス1403（図22、図23）あるいはカード内部バス1404（図24）を介して計算機内に入力されるが、この部分及び全体のパッケージ等は図22～図24に示す乱数入力装置毎に異なっている。なお、図22、図23の装置において、バス・インタフェース1401は、コンピュータ・データ入出力バス1403を介して受け取った計算機からの命令に基づき、物理乱数発生回路100から乱数データ106を取得し、要求元の計算機に送信する。

【0224】図22の場合は、乱数入力装置が基板として提供される例である。この基板形態では、物理乱数発生基板1400aをPCIバスのようなコンピュータの

スロットに挿入して使用される。

【0225】図23の場合は、乱数入力装置がカードとして提供される例である。このカード形態では、物理乱数発生カード1400bをPCMCIAのようなカード用のスロットに挿入して使用される。

【0226】図24の場合は、乱数入力装置がICカード1400cとして提供される例である。なお、ICカードはCPU（図示せず）が内蔵され一種の計算機であるとみなせるので、この場合は乱数入力装置が計算機自体に組み込まれた形になっている。

【0227】すなわちICカード1400cにはCPUが内蔵されているため（図示せず）、コンピュータ・データ入出力バス1403ではなく、カード内部バス1404を経由してICカード内部のCPUへ乱数データを出力することになる。このような形態にすることにより、セキュリティ上性質の良い乱数が必要なICカードを実現することができる。

【0228】上述したように、本発明の実施の形態に係る物理乱数発生装置を用いた乱数入力装置においては、計算機への乱数入力に物理乱数発生回路100からの乱数データ106を利用するようにしたので、装置の小型化、低価格化を実現させることができる。

【0229】また特に、コンピュータの入出力バスとして、PCIバスのような汎用性のあるバスを用いれば、1品種の基板の開発により、パソコンのような小さな計算機からEWSや並列計算機まで対応することができるようになり、大量生産が可能になる。これにより本発明の目的である低価格化がより効果的に実現される。

【0230】（発明の第20の実施の形態）本実施形態では、1個の物理乱数発生装置をネットワークに接続して、複数の計算機に乱数データを供給することを可能にする。

【0231】図25は本発明の第20の実施の形態に係る物理乱数発生装置の構成例を示すブロック図である。

【0232】この物理乱数発生装置は、物理乱数発生回路100及びネットワーク・インターフェイス1501から構成されている。なお、物理乱数発生回路100は、第1～第15の実施形態で説明した物理乱数発生装置の何れかと同様に構成されている。

【0233】ネットワーク・インターフェイス1501は、ネットワーク・ケーブル1502を介して受け取った命令にもとづき、物理乱数発生回路100から乱数データ106を取得し、ネットワークに送信する。

【0234】上述したように、本発明の実施の形態に係る物理乱数発生装置においては、ネットワークに提供する乱数に、物理乱数発生回路100からの乱数データ106を利用するようにしたので、安価に複数の計算機において物理乱数を利用することができる。

【0235】すなわち、1台の専用物理乱数発生装置から複数の計算機にデータを供給するため、計算機1台あ

たり物理乱数発生に関わる単価を低く抑えることができる。そのため、本発明の目的である低価格化を実現することができる。

【0236】（発明の第21の実施の形態）本実施形態では、物理乱数データの要求に対する供給を安定化する記録再生機能付きの物理乱数発生装置について説明する。

【0237】特に、乱数データを要求する相手が計算機の場合、乱数データだけを高速に要求する可能性は小さく、乱数データの要求を行う間にいくつかの演算を行うため、物理乱数発生装置の乱数データ供給が過剰になることが多い。

【0238】そこで、本実施形態の物理乱数発生装置は、たとえば物理乱数データの要求が少ない夜間に乱数データを記憶装置に記録しておき、要求に対する乱数データの供給を記憶装置から行うことにより、記憶装置の容量までの要求に対して十分に高速に乱数データの提供を可能とするものである。

【0239】図26は本発明の第21の実施の形態に係る物理乱数発生装置の構成例を示すブロック図である。

【0240】この記録再生機能付きの物理乱数発生装置は、物理乱数発生回路100、記憶装置インターフェイス1601及び記憶装置1604より構成されている。なお、物理乱数発生回路100は、第1～第15の実施形態で説明した物理乱数発生装置の何れかと同様に構成されている。

【0241】記憶装置インターフェイス1601は、乱数データ106を一旦記憶装置1604に記録し、図示しない外部装置の要求に従って、記憶装置1604から乱数データを再生して再生乱数データ1605として出力する。

【0242】上述したように、本発明の実施の形態に係る物理乱数発生装置においては、乱数の出力頻度によらずつきがあるような状態で乱数データ106を使用する場合、緩衝の役割をする記憶装置1604を用いることにより、乱数発生の要求が瞬間的に多くなっても対応することができる。

【0243】すなわち過剰に発生した乱数データを、一旦記憶装置に記録することにより、瞬間的に乱数データの要求が発生する場合の緩衝が可能になり、安定に乱数データを供給することができる。

【0244】（発明の第22の実施の形態）本実施形態では、物理乱数データをフロッピー・ディスクやCD-ROMのような記憶媒体に記録して提供することを可能とする物理乱数発生装置について説明する。

【0245】物理乱数は、周期性のない様な質の良い乱数を発生することができる反面、発生する乱数データの順序を予測できないことが利用上の課題となることがある。たとえば、送信するデータを暗号化する場合、受信側が持っている媒体に記録された内容と同じ内容を記

録した媒体を利用し、送信データと一緒に暗号化に使用した乱数データが存在する場所だけを示すデータ（解読キー）を送信することにより、第三者に全く解読されない状態で情報のやり取りができるようになる。そこで、本実施形態では第1～第15の実施形態の物理乱数発生装置の何れかで作成した物理乱数データを可搬な媒体に記録する。このための記録媒体としては、FD、MO、CD-ROM、DVD-ROM等が用いられる。

【0246】上述したように、本発明の実施の形態に係る物理乱数発生装置においては、第1～第15の実施形態の物理乱数発生装置で生成した物理乱数データを可搬な媒体に記録するようにしたので、物理乱数データを記録した媒体を通信を行う当事者間で保有することができ、第3者に知られることなくデータの暗号化／解読を行なうことができる。

【0247】これにより、ハードウェアを購入するよりもはるかに安価に乱数データを取得することができる。

【0248】（発明の第23の実施の形態）本実施形態では、第22の実施形態において乱数データの質を保証して供給するようにしたものである。

【0249】乱数の質を示すための検定手法は複数あり、乱数を使用する場合はいくつかの検定を行った上で乱数データを利用するのが一般的であるが、そのためのソフトウェア開発等の作業に要する時間は膨大になる。したがって、本実施形態では乱数の質を示す検定方法と検定結果を乱数データとともに記録した可搬な媒体を供給するようにしたものである。

【0250】本実施形態では第1～第15の実施形態の物理乱数発生装置の何れかで作成した物理乱数データを可搬な媒体に記録するとともに、当該媒体にその検定方法及び検定結果を記録する。

【0251】ここで、検定方法について説明する。

【0252】与えられた数列を乱数列と見なして良いか否かを判定するための確固たる手順は、現在のところ存在しないといってもよい。普通に使われている方法は、その数列が、一様母集団からのランダムサンプルであるという仮説を、幾つかの方法で検定し、その総合結果から判断する、というものである。

【0253】検定の種類とか、実行手順、パラメータの選択等については、検定を行う者の好みにまかされておき、標準的な検定方法さえ確立していない。

【0254】検定方法には以下のようなものがある。

【0255】まず、

- (1) 一次元、二次元、三次元の頻度検定
- (2) マルコフ性の検定

与えられた数列を、状態間の推移が等確率であるようなマルコフ過程の一つの実現値と見て、標本推移度数の等確率性を検定する。

【0256】

- (3) モーメント（平均、分散）の検定

(4) 遅れが1, 2, . . . の系列相関係数の検定

(5) 二次元、三次元のランダム距離の検定

(6) 連の検定（上昇連、下降連の長さの分布、個数の平均、符号連）
等が考えられる。

【0257】また、他の方法（日本規格協会等の乱数表の検定に用いられている伝統的な方法）として、

- (1) 一次元度数検定
- (2) 二次元度数検定（系列検定）
- (3) ボーカール検定
- (4) 連の検定（上昇連、下降連）
- (5) ギャップの検定
- (6) 衝突検定
- (7) OPSO検定

等も考えられる。

【0258】さらに、他の方法（パチンコ台用の乱数発生器）として、

- (1) 一次元度数検定
- (2) 二次元度数検定
- (3) スペクトル検定
- (4) 相関係数による検定
- (5) 自己相関係数、偏自己相関係数による検定
- (6) 連の検定

等も考えられる。

【0259】また、このための媒体としては、FD、MO、CD-ROM、DVD-ROM等が用いられる。

【0260】上述したように、本発明の実施の形態に係る物理乱数発生装置においては、第1～第15の実施形態の物理乱数発生装置で生成した物理乱数データ、その検定方法及び検定結果を可搬な媒体に記録するようにしたので、第22の実施形態と同様な効果が得られる他、その検定方法及び検定結果により、媒体に記録された乱数データの質を容易に確認することができる。

【0261】すなわち媒体に記録された乱数データを利用するユーザが改めて検定を行うことなく安心してデータを利用することができ、物理乱数の普及につながるものである。

【0262】なお、上記各実施形態の物理乱数発生装置により得られる効果を整理すると以下の通りである。

【0263】(1) 物理乱数発生速度の向上

従来の乱数発生方法が、ランダム・パルスの計数によるものであったのに対し、本発明ではノイズ源を直接サンプリングして得られる統計的分布を利用したものであるため、乱数を高速に発生することができる。

【0264】(2) ノイズ源および乱数発生処理回路の簡素化

従来の乱数発生方法では、1つのノイズ源に対して1ビットの乱数発生であったのに対し、本発明ではアナログ・デジタル変換器を用いることにより、1度に複数のビットを発生することができる。

【0265】(3) 乱数として良質な特性を有する乱数の提供

熱雑音のような統計的現象を電氣的にとらえているので、発生する乱数は自然界のランダム現象に基づくものであり、良質な特性を有する乱数の提供が可能である。

【0266】(4) 乱数発生装置の幅広い分野への適用
 計算機への応用ではパソコンから汎用コンピュータ、民生用ではゲーム機やパチンコ台、そしてICカードへの適用を行うことができる。

【0267】なお、本発明は、上記各実施の形態に限定されるものでなく、その要旨を逸脱しない範囲で種々に変形することが可能である。

【0268】また、実施形態に記載した手法は、計算機に実行させることができるプログラム（ソフトウェア手段）として、例えば磁気ディスク（フロッピーディスク、ハードディスク等）、光ディスク（CD-ROM、DVD等）、半導体メモリ等の記憶媒体に格納し、また通信媒体により伝送して頒布することもできる。なお、媒体側に格納されるプログラムには、計算機に実行させるソフトウェア手段（実行プログラムのみならずテーブルやデータ構造も含む）を計算機内に構成させる設定プログラムをも含むものである。本装置を実現する計算機は、記憶媒体に記録されたプログラムを読み込み、また場合により設定プログラムによりソフトウェア手段を構築し、このソフトウェア手段によって動作が制御されることにより上述した処理を実行する。

【0269】

【発明の効果】以上詳記したように本発明によれば、物理乱数発生速度を向上するとともに、乱数として良質な特性を有する物理乱数を提供し、汎用のコンピュータからパソコンやゲーム機のような民生レベルまで幅広い分野への適用をできるようにした物理乱数発生装置及び方法、物理乱数入力装置並びに物理乱数記録媒体を提供することができる。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態に係る物理乱数発生装置の構成例を示すブロック図。

【図2】同実施形態の物理乱数発生装置におけるAC結合増幅器の内部構成例を示す図。

【図3】ノイズ信号波形の例を示す図。

【図4】本発明の第2の実施の形態に係る物理乱数発生装置の構成例を示すブロック図。

【図5】本発明の第3の実施の形態に係る物理乱数発生装置の構成例を示すブロック図。

【図6】本発明の第4の実施の形態に係る物理乱数発生装置の構成例を示すブロック図。

【図7】オフセット及びゲイン変動に対する一様性に関するシミュレーション結果を示す図。

【図8】本発明の第5の実施の形態に係る物理乱数発生装置におけるA/D変換範囲を決定するためのシミュレ

ーション結果を示す図。

【図9】本発明の第6の実施の形態に係る物理乱数発生装置の構成例を示すブロック図。

【図10】本発明の第7の実施の形態に係る物理乱数発生装置の主要部の構成例を示すブロック図。

【図11】本発明の第8の実施の形態に係る物理乱数発生装置の主要部の構成例を示すブロック図。

【図12】本発明の第9の実施の形態に係る物理乱数発生装置におけるノイズ源の一例を示す構成図。

【図13】本発明の第10の実施の形態に係る物理乱数発生装置におけるノイズ源の一例を示す構成図。

【図14】本発明の第11の実施の形態に係る物理乱数発生装置におけるノイズ源の一例を示す構成図。

【図15】本発明の第12の実施の形態に係る物理乱数発生装置におけるノイズ源の一例を示す構成図。

【図16】本発明の第13の実施の形態に係る物理乱数発生装置におけるノイズ源の一例を示す構成図。

【図17】本発明の第14の実施の形態に係る物理乱数発生装置におけるノイズ源の一例を示す構成図。

【図18】本発明の第15の実施の形態に係る物理乱数発生装置におけるノイズ源恒温化装置の一例を示す構成図。

【図19】本発明の第16の実施の形態に係る物理乱数発生装置を用いた表示装置の構成例を示すブロック図。

【図20】本発明の第17の実施の形態に係る物理乱数発生装置を用いた通信装置の構成例を示すブロック図。

【図21】本発明の第18の実施の形態に係る物理乱数発生装置を用いたデータ暗号化装置の構成例を示すブロック図。

【図22】本発明の第19の実施の形態に係る物理乱数発生装置を用いた乱数入力装置の一構成例を示すブロック図。

【図23】同実施形態の物理乱数発生装置を用いた乱数入力装置の他の構成例を示すブロック図。

【図24】同実施形態の物理乱数発生装置を用いた乱数入力装置のさらに他の構成例を示すブロック図。

【図25】本発明の第20の実施の形態に係る物理乱数発生装置の構成例を示すブロック図。

【図26】本発明の第21の実施の形態に係る物理乱数発生装置の構成例を示すブロック図。

【符号の説明】

101…ノイズ源

103…AC結合増幅器

105…アナログ・デジタル変換器

106…乱数データ

201…オフセット検出器

203…デジタル・アナログ変換器

205…デジタル加算器

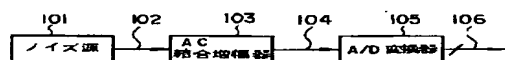
401…アナログ・デジタル変換器の変換範囲

402…オーバーフロー範囲

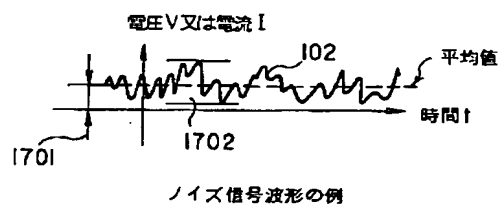
403…アンダーフロー範囲
 404…オーバーレンジ範囲
 502…オーバーレンジ処理器
 601, 602…抵抗
 603, 604…ヒータ
 701, 702, 704, 705, 707…抵抗
 703…トランジスタ
 706…ツェナーダイオード
 801…フォトマルチプライヤ
 806, 807, 808…バイアス印加用の抵抗
 809…高圧電源
 901…2極真空管
 905…バイアス印加用の抵抗
 906…高圧電源
 907…ヒータ電源
 1001…真空マイクロ素子
 1005…バイアス印加用の抵抗
 1006…高圧電源
 1007…制御電源
 1101…表示処理器
 1103…表示器
 1104…制御パネル
 1201…変調信号発生器

1203…変調器
 1302…暗号化装置
 1401…バス・インタフェース
 1403…コンピュータ・データ入出力バス
 1404…カード内部バス
 1501…ネットワーク・インターフェイス
 1502…ネットワーク・ケーブル
 1601…記憶装置インターフェイス
 1602…記憶装置
 1801…入力コンデンサ
 1802…増幅器
 1803…出力コンデンサ
 2001…ノイズ源素子
 2002…恒温ケース
 2003…ヒータ
 2005…恒温制御器
 2101…補正信号発生器
 2103…ディジタル・アナログ変換器
 2105…ディジタル減算器
 2106…加算器
 2201…レジスタ
 2202…レジスタ
 2203…ディジタル加算器

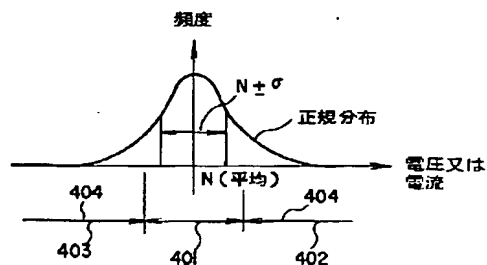
【図1】



【図3】

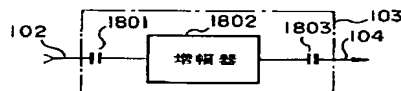


【図8】

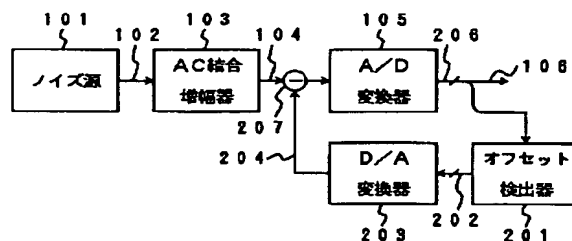


ディジタル値の頻度分布とADCの変換範囲

【図2】

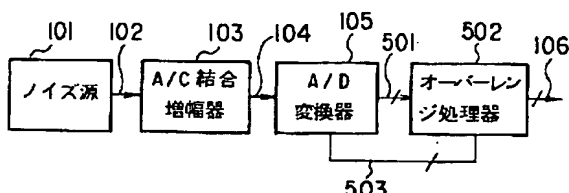


【図4】



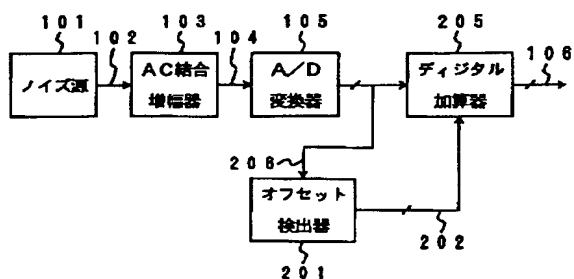
アナログ信号によるオフセット調整

【図9】

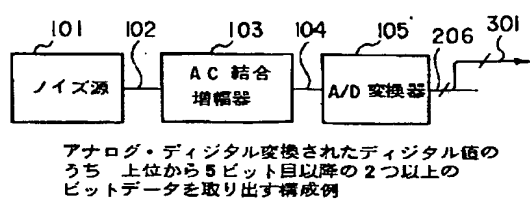


ADCの入力範囲を超えた場合の処理機能を有する物理乱数発生装置の構成例

【图5】

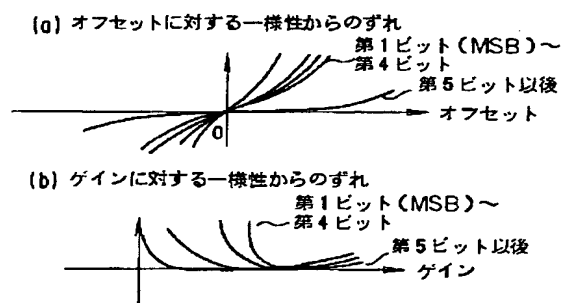


【図 6】



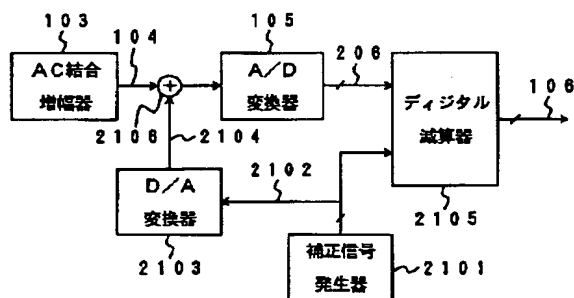
アナログ・ディジタル変換されたディジタル値のうち 上位から5ビット目以降の2つ以上のビットデータを取り出す構成例

【図 7】



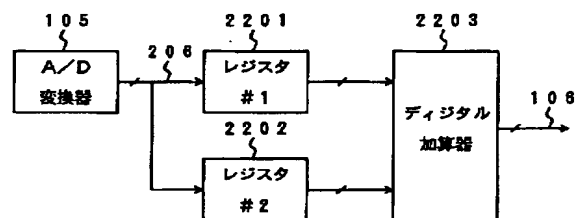
オフセットおよびゲイン変動に対する一様性

【図 10】

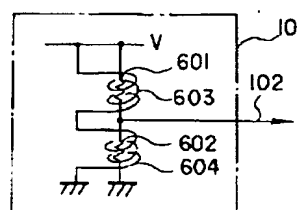


微分非直線性を改善した物乱数発生装置の構成例

【图 1 1】

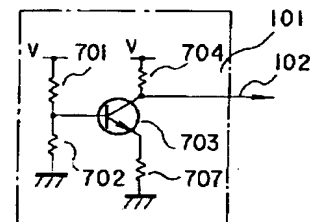
加算平均化により微分非直線性の影響を改善した
物理乱数発生装置の構成例

【图 1 2】



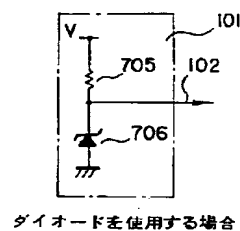
抵抗の熱雑音をノイズ源とする場合の構成例 トランジスタを使用する場合

【图 13】



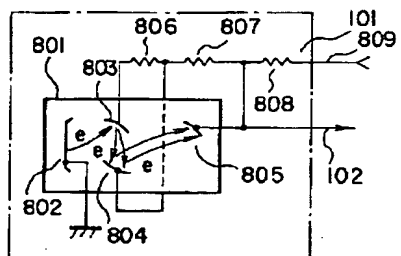
【图 16】

【图 14】

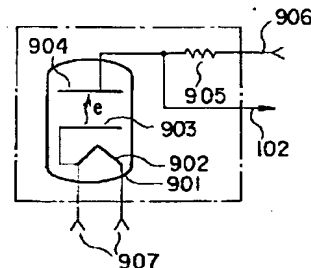


ダイオードを使用する場合

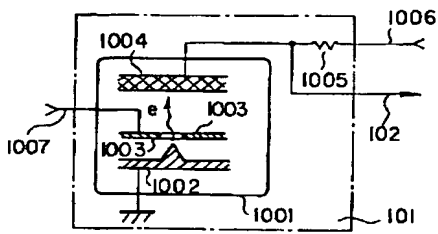
【图 15】



フォトマルチプライヤをノイズ源とする場合の構成例 真空管をノイズ源とする場合の構成例

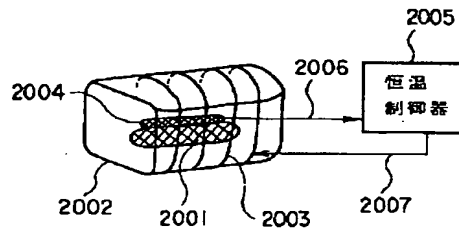


【図17】



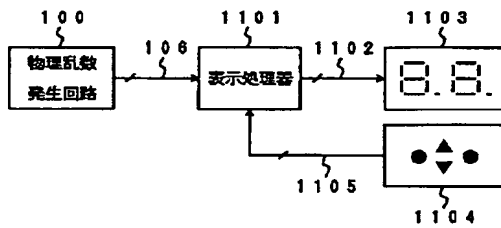
真空マイクロ素子をノイズ源とする場合の構成例

【図18】



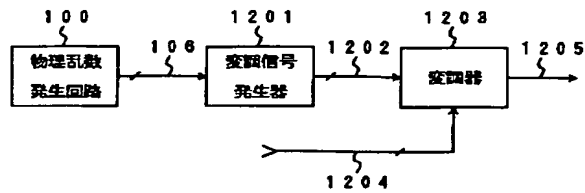
ノイズ源の恒温化の例

【図19】



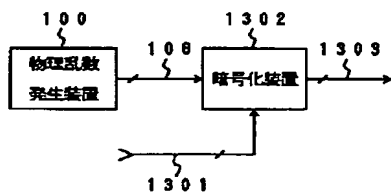
乱数データの表示機能付物理乱数発生装置の構成例

【図20】



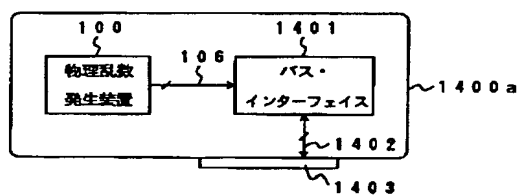
乱数データによる変調機能付物理乱数発生装置の構成例

【図21】



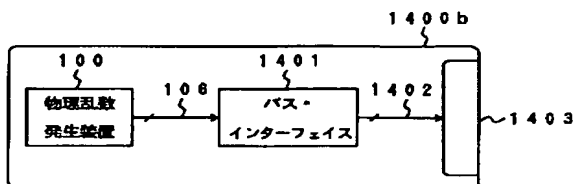
乱数データによる暗号化機能付物理乱数発生装置の構成例

【図22】



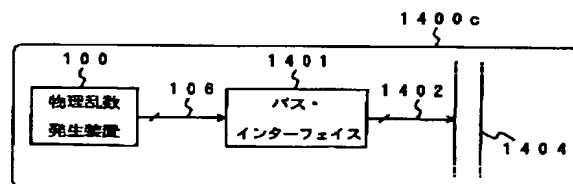
基板形態の例

【図23】



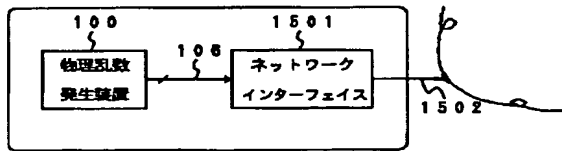
カード形態の例

【図24】



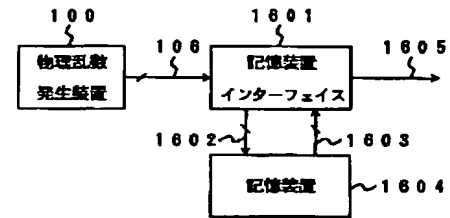
ICカード形態の例

【図25】



コンピュータ・ネットワークへの接続機能付物理乱数発生装置例

【図26】



記録再生機能付物理乱数発生装置例

フロントページの続き

(56) 参考文献 特開 平9-97170 (JP, A)
 特開 平5-80987 (JP, A)
 特開 平6-259233 (JP, A)
 特開 平6-168210 (JP, A)
 特開 平4-140947 (JP, A)

(58) 調査した分野(Int. Cl. 6, DB名)
 G06F 7/58
 G09C 1/00 650
 H04L 9/26
 H03K 3/84
 H03B 29/00